REMARKS

Claims 1-3, 6-8 and 28 have been amended. Claims 9-27 have been cancelled. Claims 1-8 and 28-30 are pending and presented for examination.

In this Response, Applicants have cancelled claims 9-27 from further consideration in this application. Applicants are not conceding that the subject matter encompassed by claims 9-27 is not patentable. Claims 9-27 were cancelled in this Response solely to facilitate expeditious prosecution of the remaining claims. Applicants respectfully reserve the right to pursue additional claims, including the subject matter encompassed by claims 9-27, as presented prior to this Response, in one or more continuing applications.

Information Disclosure Statement

In the present Office action, the Examiner indicated that some of the references cited in the Information Disclosure Statement filed March 18, 2004 and in the Supplemental Disclosure Statement filed February 25, 2008, were not considered due to informalities. In a telephonic conference with the undersigned's assistant, the Examiner indicated that he was unable to retrieve some of the foreign references cited from PAIR, however, upon a search of PAIR, it was found that the references were stored and were legible copies of the references filed with both IDSs. The Examiner indicated that it was an internal glitch, and he could not retrieve the references from PAIR. Additionally, the US Publications that were filed with the IDS on March 18, 2004 were listed under the incorrect section of Form 1449. Although the Examiner agreed to consider the references, as listed, he suggested that, for clarity's sake, a "corrected" IDS be filed listing the US Publications and the foreign references on the Form PTO-1449. Applicants hereby submit, under separate cover, a corrected IDS per the Examiner's request. Applicants, additionally, request that the Examiner consider the references submitted in the IDS and that they

be made of record. The Examiner also indicated that there would not be a fee associated with filing the corrected IDS.

Claims Objections

The Examiner objected to claims 1, 2, 6, 9, 14, 17, 18, 20, 21, 24, 25, 27, 28 and 29 due to informalities. Applicants respectfully traverse this rejection.

It is respectfully submitted that Applicants are not claiming a device capable of providing a level of security, rather Applicants are claiming a method wherein certain claimed features determine if a remote device is capable of providing a level of security. As such, Applicants respectfully request the claim objections be withdrawn.

Claims Rejections

The Examiner rejected claims 1-5, 9-13, 17-20 and 24-30 under 35 U.S.C. 102(e) as being anticipated by US Publication 2004/0139322A1 ***(Kaler)***. Applicants respectfully traverse this rejection.

The Examiner rejected claims 6-8, 14-16 and 21-23 under 35 U.S.C. 103(a) as being unpatentable over ***Kaler*** in view of US Publication 2004/0139352 ***(Shewchuk)***. Applicants respectfully traverse this rejection.

Rejections under 35 U.S.C. §102

For ease of discussion, claim 1 is discussed first. Claim 1, directed to a method, calls for (1) determining security information associated with at least one object of a transaction, wherein the object is to be transmitted from a source device to a target device along a transmission path that includes at least one intermediate device, (2) determining if an adjacent intermediate device in the transmission path is capable of providing a level of security indicated by at least a portion

of the security information, and (3) transmitting the object to the adjacent intermediate device in the transmission path in response to determining that the adjacent intermediate device is capable of providing the level of security. By detecting the level of security at each hop along a transmission path, the sender of an object, by way of a non-limiting, illustrative example, can ensure that a desired level of security is maintained throughout the transmission of the object. This may be desirable for transmissions of sensitive/personal information, for example.

The Examiner's rejection fails because ***Kaler*** fails to teach one or more of the claimed features. For instance, the ***Kaler*** reference at least does not teach the claimed feature of determining if an adjacent intermediate device in the transmission path is capable of providing a level of security indicated by at least a portion of the security information. Specifically, as stated by the Examiner on page 4 of the Office Action, a first and second end message processor establish a secure context with each other. *See* ***Kaler***, ¶[0019]. Thus, ***Kaler*** teaches establishing a secure context between endpoints of a transmission (*i.e.,* the source and target, as taught in claim 1). ***Kaler***, however, is not concerned with any intermediate (intervening) devices in the transmission path because ***Kaler*** abstracts its security measures to the application layer during the transmission (*i.e.,* not at lower level layers involved in transport such as the transport layer, the network layer, the data link layer or the physical layer). *See, e.g.,* ***Kaler***, ¶[0016], ¶[0020] and Abstract. Using this abstraction, intermediate (intervening) devices in a transmission path would not be handling any data in a packet that needs security during a transmission, and therefore, by ***Kaler's*** teaching, there is no reason to check security levels for an intermediate (intervening) device. *See* ***Kaler***, Fig. 2 and ¶[0020]. Fig. 2 in ***Kaler*** specifically shows a secure context between endpoints wherein the security level of Intermediary Message Processors 206 & 207 is ignored. *See* ***Kaler***, Fig. 2. As such, ***Kaler*** cannot, and does not, teach determining if an

adjacent intermediate remote device in the transmission path is capable of providing a level of security indicated by at least a portion of the security information, as taught in claim 1 of the instant Application.

For similar reasons, ***Kaler*** does not teach the claimed feature of transmitting the object to the adjacent intermediate device in the transmission path in response to determining that the adjacent intermediate device is capable of providing the level of security. As discussed above, ***Kaler*** is not concerned with determining the security level of devices along the transmission path, only endpoints are of concern. In fact, the teachings in ***Kaler*** are specifically intended to ignore intervening security levels by its application layer abstraction.

It is respectfully submitted that ***Kaler*** actually *teaches away* from the claimed feature because, as noted above and in the ***Kaler*** reference, intervening devices along a transmission path are ignored for security purposes. As such, the subject matter of the instant Application and the teachings of ***Kaler*** are incompatible.

For at least the aforementioned reasons, claim 1, and its dependent claims, are allowable. For similar reasons, claim 28, and its dependent claims, are also allowable.

Other claims are allowable for addition features recited therein. For example, method claim 2, which depends from claim 1, calls for receiving a response from the adjacent intermediate device in the transmission path indicating that the adjacent intermediate device in the transmission path is capable of providing the desired level of security. As discussed above, ***Kaler*** is not concerned with determining the security level of devices along the transmission path, thus the adjacent intermediate device in the transmission path would not send a response, to be received by the current holder of the object, regarding an inquiry into the security level of the adjacent intermediate device. The Examiner's references to ***Kaler*** do not support an anticipation

argument. Kaler describes establishing a secure context between the two endpoints of a transmission at the application layer. For this reason, system described in Kaler is not concerned with ensuring that any of the intermediate devices between the two endpoints is capable of providing the desired level of security. Indeed, the ***Kaler*** system is agnostic to how many or what kind of devices are between the endpoints since it is based on a security that is abstracted to the application layer. In contrast, claim 2 calls for receiving a response from the adjacent intermediate device in the transmission path indicating that the adjacent intermediate device in the transmission path is capable of providing the desired level of security.

Claim 2 also calls for the object to be a business object. The Examiner does not give any reasoning as to how the ***Kaler*** reference anticipates this claimed feature. *See* Office Action, p.4-5. ***Kaler*** is actually completely silent regarding business objects or business applications of the ***Kaler*** teachings. Business objects, as a non-limiting, illustrative example, are objects related to business processes and may require extra security because they often contain personal/identity information regarding a business transaction. *See* Application, p.12, ll. 15-16 (stating an example of a business object may be a customer invoice account). The parties sending such business objects may require extra security throughout the entire transmission path.

For at least these reasons, claim 2 is allowable.

Claim 3, a method depending from claim 1, is also allowable for additional reasons. Claim 3 calls for, among other things, transmitting to the adjacent intermediate device in the transmission path information representative of the level of security that is desired in order to prompt the adjacent intermediate device in the transmission path to execute at least one module that allows the adjacent intermediate device in the transmission path to provide the level of security. ***Kaler*** fails to teach this feature. The Examiner argues that this feature is taught by

Kaler in ¶[0086]. *See* Office Action, p.12. Specifically, the Examiner points to the teaching of ***Kaler*** describing functional result-oriented step for exchanging information. *See* ***Kaler,*** ¶[0086]. This paragraph in ***Kaler*** teaches that "any corresponding acts for accomplishing the result of exchanging information." *Id.* Fig. 3 in ***Kaler***, and the surrounding context of ¶[0086], make it clear that "information" refers to "context information. *See* ***Kaler***, Fig. 3. Thus, the Examiner's rejection fails because the claimed feature of transmitting to the adjacent intermediate device in the transmission path information representative of the level of security that is desired in order to prompt the adjacent intermediate device in the transmission path to execute at least one module that allows the adjacent intermediate device in the transmission path to provide the level of security does **not** call for an exchange of context information.

In fact, ***Kaler*** actually *teaches away* from the claimed feature because prompting the adjacent intermediate device to execute a module allowing it provide a desired level of security allows for the exchange of actual information, not context information. That is, executing a module does not enable the adjacent intermediate device to transfer security information/status. The adjacent intermediate device could transfer security information without the execution of the module. However, in order to receive and transmit the object, the adjacent intermediate device needs to execute at least one module in order to perform at the desired level of security.

Claim 3 also calls for comparing the adjacent intermediate device in the transmission path to a list of trusted devices in the header portion of the object. The cited references are silent regarding this feature. By allowing the adjacent intermediate device to be on a trusted device list, a comparison and subsequent match of the adjacent intermediate device may allow a quicker, more efficient overall transmission of the object.

Claim 3 further calls for transmitting the object to a "business integration adapter" handler module that supports several different connections types with other devices, as well as different connectivity options. The handler module allows for specific handling of the object in accordance with the object's security requirements. Again both cited references are silent regarding this feature.

For at least the aforementioned reasons, claim 3 is allowable.

Rejections under 35 U.S.C. §103

Claim 6, which depends from claim 1, calls for determining an alternative device that is capable of providing the level of security represented in response to determining that the adjacent intermediate device is not capable of providing the level of security. By allowing transmission to a different device, in the even the adjacent intermediate device in the transmission path is not capable of providing the desired security level, the sender of the object to find a secure path to the destination.

The Examiner's rejection fails because ***Kaler*** and ***Shewchuk***, alone or in combination, fail to teach at least one of the claimed features. The Examiner attempts to apply ***Shewchuk*** to teach the feature of determining an alternate route for the object in the event that the adjacent intermediate device cannot meet the security features, as taught in dependent claim 6. *See* Office Action, p.11-12. ***Shewchuk***, however, fails to teach this feature. ***Shewchuk***, as cited by the Examiner, teaches a requesting client first communicates with a validating message processor to establish an encapsulated security token. *See* ***Shewchuk***, ¶¶[0115]-[0116] and Fig. 5. Once established, the client then sends an encapsulated security token to a server in order to create a secure relationship. *Id.* In other words, the client must first go to one server in order to encapsulate his token, then the client goes to another server to establish a trusted relationship.

As such, ***Shewchuk*** does not teach an alternate route is chosen in response to determining that the adjacent intermediate device is not capable of providing the level of security. ***Shewchuk*** does not teach an alternative path because going to a first server then to a second server is the desired path taught. Likewise, because it is the desired path taken, there cannot be an alternate route chosen. It is respectfully submitted that the Examiner is misapplying ***Shewchuk*** to claim 6. ***Kaler*** fails to remedy the fundamental deficiencies of ***Shewchuk***.

For at least the aforementioned reasons, claim 6 is allowable.

Similarly, it is respectfully submitted that the Examiner is misapplying the ***Kaler*** reference to claim 7. Claim 7, which depends from claim 1, calls for sending a message to the adjacent intermediate remote device that instructs the adjacent intermediate device to execute at least one module that allows the adjacent intermediate device to provide the level of security. As discussed above, with respect to claim 3, ***Kaler*** actually teaches away from the claimed feature because causing the adjacent intermediate device to execute a module allowing it provide a desired level of security allows for the exchange of actual information, not context information. That is, executing a module does not enable the adjacent intermediate device to transfer security information/status. The adjacent intermediate device could transfer security information without the execution of the module. However, in order to receive and transmit the object, the adjacent intermediate device must execute at least one module in order to perform at the desired level of security. ***Shewchuk*** fails to remedy the fundamental deficiencies of ***Kaler***.

For at least the aforementioned reasons, claim 7 is allowable.

Applicants respectfully assert that ***Kaler***, ***Shewchuk***, and/or their combination do not teach or disclose all of the elements of claims 6-8 of the present invention. In order to establish a prima facie case of obviousness, the Examiner must consider the following factors: 1) there must

be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine the teachings; 2) there must be a reasonable expectation of success; and 3) the prior art reference(s) must teach or suggest all the claim limitations. MPEP § 2143 (2005) (citing *In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991). In making an obviousness rejection, it is necessary for the Examiner to identify the reason why a person of ordinary skill in the art would have combined the prior art references in the manner set forth in the claims. *KSR Int'l Co. v. Teleflex, Inc.*, at 14, No. 04-1350 (U.S. 2007). Applicants respectfully submit that the Examiner has not met this burden. If in fact, as illustrated below, ***Kaler*** and ***Shewchuk*** are incompatible, and consequently those skilled in art would not combine them and make all of the elements of claims of the present invention obvious. ***Kaler*** and ***Shewchuk*** are directed toward two very different methods of establishing security. ***Kaler*** describes establishing a secure context between endpoints, and ***Shewchuk*** teaches client server trust relationships using security token protocols. One skilled in the art would not combine and endpoint based methodology with a server/token based methodology because endpoint-to-endpoint security is designed such that interaction with a server is not necessary. The endpoints may communicate directly with each other and establish a secure context independently over a network. Accordingly, Applicants respectfully submit that a *prima facie* case of obviousness has not been established in rejecting claims 6-8.

Applicants respectfully assert that in light of the amendments and arguments provided throughout the prosecution of the present application, all claims of the present application are now allowable and, therefore, request that a Notice of Allowance be issued. Reconsideration of the present application is respectfully requested.

If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is respectfully requested to call the undersigned attorney at the Houston, Texas telephone number (713) 934-4064 to discuss the steps necessary for placing the application in condition for allowance.

Respectfully submitted,

WILLIAMS, MORGAN & AMERSON, P.C.
CUSTOMER NO. 23720

Date: July 7, 2008

By: /Ruben S. Bains/
Ruben S. Bains, Reg. No. 46,532
10333 Richmond, Suite 1100
Houston, Texas 77042
(713) 934-4064
(713) 934-7011 (facsimile)
ATTORNEY FOR APPLICANT(S)